MASON LLP
Danielle L. Perry (SBN 292120)
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Telephone: 202-429-2290
Email: dperry@masonllp.com

Counsel for Plaintiff and the Proposed Class
[Additional counsel appear on signature page]

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

DAWN PITTINGER, individually and on behalf of all other similarly situated,

Plaintiff,

v.

CEREBRAL INC., a Delaware corporation,

Defendant.

Case No.: 2:23-cv-2043

CLASS ACTION COMPLAINT FOR:
1. NEGLIGENCE
2. NEGLIGENCE *PER SE*
3. BREACH OF IMPLIED CONTRACT
4. BREACH OF FIDUCIARY DUTY
5. UNJUST ENRICHMENT
6. DECLARATORY JUDGMENT
7. CALIFORNIA CONSUMER PRIVACY ACT
8. CALIFORNI CONSUMER RECORDS ACT
9. CALIFORNIA UNFAIR COMPETITION LAW
10. CALIFORNIA INVASION OF PRIVACY

JURY TRIAL DEMANDED

Plaintiff Dawn Pittinger ("Plaintiff"), individually and on behalf of all others similarly situated, makes the following allegations upon information and belief, except as to her own actions, the investigation of counsel, and facts that are a matter of public record.

SUBJECT MATTER JURISDICTION

1. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because this is a class action wherein the amount of

controversy exceeds the sum or value of $5,000,000 exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

NATURE OF THE ACTION

2. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant Cerebral (the "Data Breach"), which held in its possession certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, "the Private Information") of Plaintiff and other patients of Defendant Cerebral, the putative class members ("Class"). According to its notice letters to state Attorneys General and victims of the breach, this Data Breach occurred around January 3, 2023.

3. The Private Information compromised in the Data Breach included certain personal or protected health information of current and former patients, including Plaintiff. This Private Information included, but is not limited to: names, phone numbers, email addresses, dates of birth, IP address, Cerebral client ID numbers, insurance co-pay amounts, subscription type, booking information, treatment information, health insurance information and other demographic or information.

4. The Private Information compromised in what Defendant Cerebral refers to as a "HIPAA Privacy Breach" in which it "recently discovered issue related to inadvertent information sharing."[1] In other words, the cybercriminals intentionally targeted Defendant Cerebral for the highly sensitive Private Information it stores on its computer network, attacked the insufficiently secured network, then exfiltrated highly sensitive PII and PHI. As a result, the Private Information of Plaintiff and Class remains in the hands of those cyber-criminals.

5. The Data Breach was a direct result of Defendant Cerebral's failure to implement adequate and reasonable cyber-security procedures and protocols

[1] *See* Plaintiff Notice Letter, attached as Exhibit A.

necessary to protect individuals' Private Information with which it was entrusted for either treatment or employment or both.

6. Defendant Cerebral utilized poor data privacy practices, which it had been aware of and criticized for many months before about the dangers of using pixel technologies. They utilized this free technology which tracked and shared the data of PII and PHI of patients with other companies like Facebook and Google.[2]

7. In fact, the Senate questioned Defendant Cerebral on its poor practices regarding its patients' Private Information. According to a letter writing to the CEO of Defendant Cerebral, "On November 30th, 2022, a spokesperson for your company wrote in an email, "We are removing any personally identifiable information, including name, date of birth, and zip code from being collected by the Meta Pixel." As of December 7, 2022, your site was still collecting personally identifiable information."[3]

8. Defendant Cerebral revealed that after reviewing its data sharing practices, that it determined on January 3, 2023 that it disclosed PHI to subcontractors "without having obtained HIPAA-required assurances."[4]

9. Plaintiff bring this class action lawsuit on behalf of themselves and all others similarly situated to address Defendant Cerebral's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and including in that notice precisely what specific types of information

[2] *See* https://medcitynews.com/2023/03/cerebral-admits-that-it-wrongly-shared-data-of-3-1m-users/; https://www.klobuchar.senate.gov/public/_cache/files/2/e/2e36adce-7c6a-491f-87e6-a42262e16b65/CF3D6D0CF2D853FD17E1916DA2D95551.health-data-privacy-letter-to-cerebral.pdf; https://healthitsecurity.com/news/cerebral-notifies-3.1m-users-of-healthcare-data-breach-stemming-from-pixel-use

[3] *See* https://www.klobuchar.senate.gov/public/_cache/files/2/e/2e36adce-7c6a-491f-87e6-a42262e16b65/CF3D6D0CF2D853FD17E1916DA2D95551.health-data-privacy-letter-to-cerebral.pdf

[4] *Id.*

were accessed and taken by cybercriminals.

10. Defendant Cerebral maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant Cerebral's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant Cerebral, and thus Defendant Cerebral was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

11. Defendant Cerebral disregarded the rights of Plaintiff and Class Members (defined below) by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members with prompt and full notice of the Data Breach.

12. In addition, Defendant Cerebral failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant Cerebral properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals almost a month of unimpeded access to the PII and PHI of Plaintiff Class Members.

13. Plaintiff's and Class Members' identities are now at risk because of Defendant Cerebral's negligent conduct since the Private Information that Defendant Cerebral collected and maintained is now in the hands of data thieves.

14. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial

accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

15. As a result of the Data Breach, Plaintiff and Class mMembers have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and for years into the future closely monitor their financial accounts to guard against identity theft.

16. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

18. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence per se, (iii) breach of implied contract, (iv) breach of fiduciary duty; and (v) unjust enrichment, (vi) declaratory relief, (vii) California Consumer Privacy Act, (vii) California Consumer Records Act, (ix) California Unfair Competition Law, and (x) California Invasion of Privacy Act.

19. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant Cerebral, and declaratory relief.

PARTIES

20. Plaintiff Dawn Pittinger is and at all times mentioned herein was an individual citizen of the State of West Virginia, residing in the city of Orma (Calhoun County), and was a patient of Defendant Cerebral.

21. Defendant Cerebral Inc is a corporation organized and existing undert the laws of the State of Delaware, whose principal place of business is located at 340 South Lemon Avenue, Suite 9892, Walnut, California 91789.

PERSONAL JURISDICTION AND VENUE

22. The Court has general personal jurisdiction over Defendant Cerebral because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in this State; it is registered with the Secretary of State as a for-profit corporation; it maintains its headquarters in California; and committed tortious acts in California.

23. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which Defendant Cerebral has the most significant contacts.

FACTUAL ALLEGATIONS

Defendant's Business

24. Defendant Cerebral is a startup telehealth company headquartered in California, which has been providing mental health services virtually throughout the U.S.[5] It claims to provide affordable mental health care with the highest quality of care by following a clinical code of ethics. One code which includes using "the latest information security technology to protect your data, which is not shared without your consent, and will only be used internally to improve clinical care."[6]

25. Defendant Cerebral "offers long-term online care and medication management for a wide range of mental health conditions."[7]

---

[5] https://cerebral.com/about-cerebral (last accessed Mar. 13, 2023).
[6] *Id.*
[7] *See* https://cerebral.com/faqs#General_questions-How_does_Cerebral_work_ (last visited Mar. 13, 2023).

26. For the purposes of this Class Action Complaint, all of Defendant Cerebral's associated locations will be referred to collectively as "Cerebral."

27. In the ordinary course of receiving medical care services from Defendant Cerebral, each patient and employee must provide (and Plaintiff did provide) Defendant Cerebral with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;
- Marital status;
- Employer with contact information;
- Primary and secondary insurance policy holders' name, address, date of birth, and Social Security number;
- Demographic information;
- Driver license or state or federal identification;
- Information relating to the individual's medical and medical history;
- Insurance information and coverage; and
- Banking and/or credit card information.

28. Defendant Cerebral also creates and stores medical records and other protected health information for its patients, including records of treatments and diagnoses.

29. Upon information and belief, Defendant Cerebral's HIPAA Privacy Policy is provided to every patient both prior to receiving treatment and upon request.

30. Defendant Cerebral agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws,

including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA").

31. Yet, through its failure to properly secure the Private Information of Plaintiff and Class, Defendant Cerebral has not adhered to its own promises of patient rights.

32. The patient (and upon information and belief, employee) information held by Defendant Cerebral in its computer system and network included the highly sensitive Private Information of Plaintiff and Class Members.

The Data Breach

33. A data breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant Cerebral.

34. Defendant Cerebral utilized pixels "and similar common technologies ("Tracking Technologies"), such as those made available by Google, Meta (Facebook), TikTok, and other third parties ("Third Party Platforms"), on Defendant Cerebral's Platforms. Defendant Cerebral has used Tracking Technologies since [it] began operations on October 12, 2019. Cerebral recently initiated a review of its use of Tracking Technologies and data sharing practices involving Subcontractors."[8]

35. After its review "On January 3, 2023, Cerebral determined that it had disclosed certain information that may be regulated as protected health information ("PHI") under HIPAA to certain Third Party Platforms and some Subcontractors without having obtained HIPAA-required assurances."[9]

36. Defendant Cerebral's investigation found that "the information disclosed may have included your name, phone number, email address, date of birth, IP address, Cerebral client ID number, and other demographic or

[8] *See* Notice Letter, Exhibit A.
[9] *Id.*

information." Additionally, if a patient "also completed any portion of Cerebral's online mental health self-assessment, the information disclosed may also have included your selected service, assessment responses, and certain associated health information." Lastly, if a patient purchased a subscription plan, "he information disclosed may also have included subscription plan type, appointment dates and other booking information, treatment, and other clinical information, health insurance/ pharmacy benefit information (for example, plan name and group/ member numbers), and insurance co-pay amount.[10]

37. However, without further explanation, in its website notice letter Defendant Cerebral claims that "Upon learning of this issue, Cerebral promptly disabled, reconfigured, and/or removed the Tracking Technologies on Cerebral's Platforms to prevent any such disclosures in the future and discontinued or disabled data sharing with any Subcontractors not able to meet all HIPAA requirements.."[11] Then Defendant Cerebral claims to "have enhanced [its] security practices..." [12]

38. As reported to Department of Health and Human Services Office for Civil Rights ("DHH Report") on March 1, 2023, Defendant Cerebral's investigation revealed that the Private Information (including both PII and PHI) of 3,179,835 individuals was accessed in this Data Breach.[13]

39. Defendant Cerebral disclosed the Private Information of millions of people to Facebook and Google without their knowledge or consent. This information can be used to "target advertisements for services that may be unnecessary or potentially harmful physically, psychologically, or emotionally."[14]

---

[10] *See* https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last accessed Mar. 13, 2023).
[11] *Id.*
[12] *Id.*
[13] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Mar. 13, 2023).
[14] *See* https://www.klobuchar.senate.gov/public/_cache/files/2/e/2e36adce-7c6a-491f-87e6-a42262e16b65/CF3D6D0CF2D853FD17E1916DA2D95551.health-data-privacy-letter-to-cerebral.pdf

40. Defendant Cerebral had obligations created by HIPAA, FTCA, contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

41. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

42. Plaintiff and Class Members provided this information to received medical services from Defendant Cerebral. Defendant Cerebral solicited patients to use its website for online services. Through their website or subscription plans, they were able to communication with doctors or other healthcare providers, fill out questionnaires regarding mental health, schedule appointments, receive telehealth appointments, and other mental healthcare related activities as one would in a brick and mortar healthcare institution.

The Data Breach Was a

Foreseeable Risk of which Defendant Cerebral Was on Notice.

43. It is well known that PII is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including Defendant Cerebral, are well-aware of the risk of being targeted by cybercriminals.

44. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

45. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct

financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss." [15]

46. Individuals, like Plaintiff and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

47. Data Breach victims suffer long-term consequences when their Private Information is taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

48. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[16]

49. In 2021, there were a record 1,862 data breaches, surpassing both

[15] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Mar. 13, 2023).

[16] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Mar. 13, 2023).

2020's total of 1,108 and the previous record of 1,506 set in 2017.[17]

50. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[18]

51. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

52. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."[19] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[20]

53. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant Cerebral failed to take appropriate steps to protect the PII of

[17] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed Mar. 13, 2023).
[18] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed Mar. 13, 2023).
[19] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed Mar. 13, 2023).
[20] *Id.*

Plaintiff and the proposed Class from being compromised.

Data Breaches Are Rampant in Healthcare

54. Defendant Cerebral's data security obligations were particularly important given the substantial increase in Data Breaches in the healthcare industry preceding the date of the breach.

55. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[21]

56. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[22]

57. The HIPAA Journal article goes on to explain that patient records, like those stolen from Defendant Cerebral. are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[23]

58. Data breaches such as the one experienced by Defendant Cerebral

[21] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last accessed Mar. 13, 2023).
[22] *Id.*
[23] *Id.*

have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

59. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[24]

60. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[25]

61. The significant increase in attacks in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant Cerebral.

Defendant Cerebral Fails to Comply with FTC Guidelines

62. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

63. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[26] The guidelines also recommend that businesses

[24] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last accessed Mar. 13, 2023).
[25] https://www.ahu.edu/blog/data-security-in-healthcare (last accessed Mar. 13, 2023).
[26] *Protecting Personal Information: A Guide for Business*, Federal Trade

use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[27]

64. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

65. The FTC has brought enforcement actions against businesses like Cerebral's for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

66. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

67. Defendant Cerebral failed to properly implement basic data security practices.

68. Defendant Cerebral's failure to employ reasonable and appropriate

---

Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Mar. 13, 2023).

[27] *Id.*

measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

69. Defendant Cerebral was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

70. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

71. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

72. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

73. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

74. These frameworks are existing and applicable industry standards in the healthcare industry, yet Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant's Conduct Violates HIPAA

75. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information (PHI).

76. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

77. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

78. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

79. Defendant Cerebral's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

Defendant has Breached its Obligations to Plaintiff and Class

80. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Defendant Cerebral's computer systems and its patients' data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to

the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

81. As the result of maintaining its computer systems in manner that required security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

82. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

Data Breaches Put Consumers at an Increased Risk of Fraud and Identify Theft

83. Data Breaches such as the one experiences by Defendant Cerebral's patients are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

84. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[28] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. *See* GAO chart of consumer recommendations, reproduced and attached as Exhibit B. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiff and Class) must take after a breach like Defendant Cerebral's are both time consuming and of only limited and short-term effectiveness.

85. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report").[29]

86. The FTC, like the GAO (*see* Exhibit B), recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting

[28] https://www.gao.gov/assets/gao-19-230.pdf (last accessed Mar. 13, 2023). *See* attached as Ex. B.

[29] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed Mar. 13, 2023) ("2007 GAO Report").

their credit reports.[30]

87. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

88. Identity thieves can also use Private Information to obtain a driver license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

89. Theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[31]

90. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See 2007 GAO Report, at p. 29.

91. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

[30] *See* https://www.identitytheft.gov/Steps (last accessed Mar. 13, 2023).
[31] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

92. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

93. As the HHS warns, "PHI can be exceptionally valuable when stolen and sold on a black market, as it often is. PHI, once acquired by an unauthorized individual, can be exploited via extortion, fraud, identity theft and data laundering. At least one study has identified the value of a PHI record at $1000 each."[32]

94. Furthermore, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[33] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[34] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

95. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are

[32] https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf at 2 (citations omitted) (last accessed Mar. 13, 2023).
[33] *Identity Theft and Your Social Security Number*, Social Security Administration (last accessed Mar. 13, 2023). (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Mar. 13, 2023).
[34] *Id.* at 4.

able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[35]

96. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[36]

97. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Plaintiff's Experiences

98. Plaintiff is and was a patient of Defendant Cerebral at all times relevant to this Complaint. Plaintiff received a Notice of Data Breach Letter, related to Defendant Cerebral's Data Breach that is dated March 6, 2022. *See* Exhibit A.

99. The Notice Letter that Plaintiff received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the files contained her name, phone number, email address, date of birth, IP address, Cerebral client ID number, and other demographic or information, subscription plan type, appointment dates and other booking information,

[35] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Mar. 13, 2023).

[36] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Mar. 16, 2023).

treatment, and other clinical information, health insurance/ pharmacy benefit information (for example, plan name and group/ member numbers), and insurance co-pay amount and other undisclosed information. *See* Exhibit A.

100. Plaintiff is especially alarmed by the vagueness of her stolen extremely private medical information (PHI) was identified as among the breached data on Defendant Cerebral's computer system.

101. Since the Data Breach, Plaintiff monitors her financial accounts for about an hour per week. This is more time than she spent prior to learning of Defendant Cerebral's Data Breach. Having to do this every week not only wastes her time as a result of Defendant Cerebral's negligence, but it also causes her great anxiety.

102. Starting in approximately January 2023, Plaintiff began receiving an excessive number of spam calls on the same cell phone number used at Defendant Cerebral. These calls are a distraction, must be deleted, and waste time each day. Once the Notice Letter was delivered, and given the timing of the Data Breach, she believes that the calls are related to her stolen PII.

103. In addition, Plaintiff Pittinger receives *many* spam emails and texts now, and which was not typical before the Data Breach. She cannot figure out any other explanation than that it is related to Defendant Cerebral's Data Breach which included her Private Information.

104. Plaintiff is aware that cybercriminals often sell Private Information, and one stolen, it is likely to be abused months or even years after Defendant Cerebral's Data Breach.

105. Had Plaintiff been aware that Defendant Cerebral's computer systems were not secure, she would not have entrusted Defendant Cerebral with her PII and PHI.

Plaintiff's and Class Members' Injuries

106. To date, Defendant Cerebral has done absolutely nothing to

compensate Plaintiff and Class Members for the damages they sustained in the Data Breach.

107. Defendant Cerebral has merely offered one year credit monitoring services through Experian IdentityWorksSM, a tacit admission that its failure to protect their Private Information has caused Plaintiff and Class great injuries. *See* Ex. A. These limited services are inadequate when victims are likely to face many years of identity theft.

108. Defendant Cerebral's offer fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiff's and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

109. Furthermore, Defendant Cerebral's credit monitoring offer and advice (*see* Exhibit A) to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

110. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

111. Plaintiff's and Class Members' Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

112. Plaintiff and Class were damaged in that their Private Information is now in the hands of cyber criminals, sold and potentially for sale for years into the

future.

113. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

114. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

115. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

116. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

117. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

118. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

119. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred

to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

120. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information as well as health information is not accessible online and that access to such data is password-protected.

121. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

122. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII and PHI. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, Defendant Cerebral knew of the breach for about ***2 months*** before notifying the victims yet offered no explanation of purpose for the delay. This delay violates HIPAA and other notification requirements and increases the injuries to Plaintiff and Class.

Class Action Allegations

123. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

124. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised as a result of the Data Breach discovered by Defendant Cerebral in January 2023 and for which it provided notice on or about March 2023 (the "Class").

125. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

126. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification.

127. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiff at this time, but Defendant Cerebral has provided notice to HHS that the number is approximately 3,179,835 individuals.

128. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant Cerebral unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant Cerebral failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant Cerebral's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant Cerebral's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant Cerebral owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant Cerebral breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant Cerebral knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant Cerebral's misconduct;

j. Whether Defendant Cerebral failed to provide notice of the Data Breach in a timely manner; and

k. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

129. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

130. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

131. Predominance. Defendant Cerebral has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant Cerebral's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

132. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of

conduct for Defendant Cerebral. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

133. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

134. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant Cerebral failed to timely notify the public of the Data Breach;

b. Whether Defendant Cerebral owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant Cerebral's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant Cerebral's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant Cerebral failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach;

g. Whether Defendant Cerebral failed to abide by its responsibilities under HIPAA.

135. Finally, all members of the proposed Class are readily ascertainable.

Defendant Cerebral has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant Cerebral.

CLAIMS FOR RELIEF

First Count

Negligence

(On Behalf of Plaintiff and Class Members)

136. Plaintiff re-alleges and incorporates the allegations of paragraphs 1 through 135, as if fully set forth.

137. Defendant Cerebral required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare/medical services.

138. By collecting and storing this data in Defendant Cerebral's computer property, and sharing it and using it for commercial gain, Defendant Cerebral had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant Cerebral's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

139. Defendant Cerebral owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

140. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant Cerebral and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its

systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

141. Defendant Cerebral t's duty to use reasonable security measures under HIPAA required Defendant Cerebral to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

142. In addition, Defendant Cerebral had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

143. Defendant Cerebral's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant Cerebral is bound by industry standards to protect confidential Private Information.

144. Defendant Cerebral breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant Cerebral include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

145. It was foreseeable that Defendant Cerebral's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

146. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

147. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

148. Defendant Cerebral's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

149. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant Cerebral to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

Second Count

Negligence *Per Se*

(On Behalf of Plaintiff and All Class Members)

150. Plaintiff re-alleges and incorporates the allegations of paragraphs 1 through 135, and paragraphs 137 through 149, as if fully set forth.

151. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant Cerebral had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

152. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

153. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." See definition of encryption at 45 C.F.R. § 164.304.

154. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

155. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

156. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

157. The injury and harm suffered by Plaintiff and Class Members was the

reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that they failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

158. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

Third Count

Breach of Implied Contract

(On Behalf of Plaintiff and Class Members)

159. Plaintiff re-alleges and incorporates the allegations of paragraphs 1 through 135, paragraphs 137 through 149, and paragraphs 151 through 158, as if fully set forth.

160. Plaintiff and Class Members provided their Private Information to Defendant Cerebral in exchange for Defendant Cerebral's medical services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

161. Defendant Cerebral solicited, offered, and invited Class Members to provide their Private Information as part of Defendant Cerebral's regular business practices. Plaintiff and Class Members accepted Defendant Cerebral's offers and provided their Private Information to Defendant.

162. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

163. Plaintiff and Class Members paid money to Defendant Cerebral to Defendant with the reasonable belief and expectation that Defendant Cerebra; would use part of its earnings to obtain adequate data security. Defendant Cerebral

failed to do so.

164. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant Cerebral to keep their information reasonably secure.

165. Plaintiff and Class Members would not have entrusted their Private Information to Defendant Cerebral in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

166. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant Cerebral.

167. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

168. As a direct and proximate result of Defendant Cerebral's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

169. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

170. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant Cerebral to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

Fourth Count

Breach of Fiduciary Duty

(On Behalf of Plaintiff and Class Members)

171. Plaintiff re-alleges and incorporates the allegations of paragraphs 1 through 135, paragraphs 137 through 149, paragraphs 151 through 158, and 160 paragraphs through 170, as if fully set forth.

172. In light of the special relationship between Defendant Cerebral and Plaintiff and Class Members, whereby Defendant Cerebral became guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant Cerebral did and does store.

173. Defendant Cerebral has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant Cerebral's relationship with its patients and former patients, in particular, to keep secure their Private Information.

174. Defendant Cerebral breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

175. Defendant Cerebral breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

176. Defendant Cerebral breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

177. Defendant Cerebral breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

178. As a direct and proximate result of Defendant Cerebral's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses

associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant Cerebral's possession and is subject to further unauthorized disclosures so long as Defendant Cerebral fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant Cerebral's services they received.

179. As a direct and proximate result of Defendant Cerebral's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

Fifth Count

Unjust Enrichment

(On Behalf of Plaintiff and Class Members)

180. Plaintiff re-alleges and incorporates the allegations of paragraphs 1 through 135, paragraphs 137 through 149, paragraphs 151 through 158, and paragraphs 172 through 179, as if fully set forth. This count is plead in the alternative to the breach of contract count above.

181. Upon information and belief, Defendant Cerebral funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

182. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data

security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant Cerebral.

183. Plaintiff and Class Members conferred a monetary benefit on Defendant Cerebral. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant Cerebral the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

184. Defendant Cerebral knew that Plaintiff and Class Members conferred a benefit which Defendant Cerebral accepted. Defendant Cerebral profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

185. In particular, Defendant Cerebral enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant Cerebral instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant Cerebral's decision to prioritize its own profits over the requisite security.

186. Under the principles of equity and good conscience, Defendant Cerebral should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant Cerebral failed to implement appropriate data management and security measures that are mandated by industry standards.

187. Defendant Cerebral failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

188. Defendant Cerebral acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

189. If Plaintiff and Class Members knew that Defendant Cerebral had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant Cerebral.

190. Plaintiff and Class Members have no adequate remedy at law for this count.

191. As a direct and proximate result of Defendant Cerebrals's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant Cerebrals's possession and is subject to further unauthorized disclosures so long as Defendant Cerebral fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

192. As a direct and proximate result of Defendant Cerebral's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms

of injury and/or harm.

193. Defendant Cerebral should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant Cerebral should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant Cerebral's services.

Sixth Count

Declaratory Judgment

(On Behalf of Plaintiff and Class Members)

194. Plaintiff re-alleges and incorporates the allegations of paragraphs 1 through 135, paragraphs 137 through 149, paragraphs 151 through 158, paragraphs 160 through 170, paragraphs 172 through 179, and paragraphs 181 through 193, as if fully set forth.

195. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

196. An actual controversy has arisen in the wake of the Defendant's Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Defendant Cerebral is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information.

197. Plaintiff alleges that Defendant Cerebral's data security measures remain inadequate. Plaintiff and the Class Members will continue to suffer injury because of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

198. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant Cerebral continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, HIPAA, Section 5 of the FTC Act, and various states' statutes; and

b. Defendant Cerebral continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

199. The Court also should issue corresponding prospective injunctive relief requiring Defendant Cerebral to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

200. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant Cerebral. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant Cerebral occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

201. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendant Cerebral if an injunction is issued. Among other things, if another massive data breach occurs at Defendant Cerebral, Plaintiff and Class Members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant Cerebral of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant Cerebral has pre-existing legal obligations to employ such measures.

202. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant Cerebral, thus eliminating the additional injuries that would result to Plaintiff and the millions of individuals whose Private Information would be further compromised.

Seventh Count

Violation of the California Consumer Privacy Act ("CCPA")

Cal. Civ. Code § 1798, *et seq.*

(On Behalf of Plaintiff and Class Members)

203. Plaintiff re-alleges and incorporates the allegations of paragraphs 1 through 135, paragraphs 137 through 149, paragraphs 151 through 158, paragraphs 160 through 170, paragraphs 172 through 179, paragraphs 181 through 193, and paragraphs 195 through 202, as if fully set forth.

204. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> > (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

205. Defendant Cerebral is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.

206. Plaintiff and Class Members are covered "consumers" under subdivision (g) of § 1798.140 in that they are natural persons who are California residents.

207. The personal information of Plaintiff and Class Members at issue in this lawsuit constitutes "personal information" under subdivision (a) of § 1798.150 and § 1798.81.5, in that the personal information Defendant Cerebral collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) driver license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information;(v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

208. Defendant Cerebral knew or should have known that its computer systems and data security practices were inadequate to safeguard the Class Members' personal information and that the risk of a data breach or theft was highly likely. Defendant Cerebral failed to implement and maintain reasonable

security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the Class Members. Specifically, Defendant Cerebral subjected Plaintiff's and the Class Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant Cerebral's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

209. As a direct and proximate result of Defendant Cerebral's acts, Plaintiff and the Class Members were injured and lost money or property, including but not limited to the loss of Plaintiff's and the Class Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

210. Section 1798.150(b) specifically provides that: "[n]o[prefiling]notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages." Accordingly, Plaintiff and the Class Members by way of this complaint seek actual pecuniary damages suffered as a result of Defendant Cerebral's violations described herein. Plaintiff has issued and/or will issue a notice of these alleged violations pursuant to subdivision (b) of § 1798.150 and intends to amend this complaint to seek statutory damages and injunctive relief upon expiration of the 30-day cure period pursuant to subdivsions (a)(1)(A)-(B), (a)(2), and (b) of § 1798.

Eighth Count

California Customer Records Act

(On Behalf of Plaintiff and Class Members)

211. Plaintiff re-alleges and incorporates the allegations of paragraphs 1 through 135, paragraphs 137 through 149, paragraphs 151 through

158, paragraphs 160 through 170, paragraphs 172 through 179, paragraphs 181 through 193, paragraphs 195 through 202, and paragraphs 204 through 210, as if fully set forth.

212. The California Customer Records Act, Cal. Civ. Code § 1798.81.5 (all further statutory references in this count are to the California Civil Code), provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

213. Subdivision (b) of § 1798.81.5 further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

214. Subdivision (b) of § 1798.84 provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Subdivision (e) of § 1798.84 further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

215. Plaintiff and Class Members are "customers" within the meaning of subdivision (c) of § 1798.80 and subdivision (b) of § 1798.84 because they are individuals who provided personal information to Defendant Cerebral, directly and/or indirectly, for the purpose of obtaining a service from Defendant Cerebral.

216. The personal information of Plaintiff and Class Members at issue in this lawsuit constitutes "personal information" under subdivision (d)(1) of § 1798.81.5 in that the personal information Defendant Cerebral collects and which was impacted by the cybersecurity attack includes an individual's first name or

first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) driver license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;(iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information;(v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

217. Defendant Cerebral knew or should have known that its computer systems and data security practices were inadequate to safeguard the Class Members' personal information and that the risk of a data breach or theft was highly likely. Defendant Cerebral failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the Class Members. Specifically, Defendant Cerebral failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and Class Members from unauthorized access, destruction, use, modification, or disclosure. Defendant Cerebral further subjected Plaintiff's and the Class Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant Cerebral's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

218. As a direct and proximate result of Defendant Cerebral's

violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiff and the Class Members included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the Class Members by the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

219. As a direct and proximate result of Defendant Cerebral's acts or omissions, Plaintiff and the Class Members were injured and lost money or property including, but not limited to, the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to subdivision (b) of § 1798.84.

220. Section § 1798.82 further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

221. Any person or business that is required to issue a security breach notification under the California Customer Records Act must meet the following requirements under subdivision (d) of § 1798.82:

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

i. the date of the breach,

ii. the estimated date of the breach, or

iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

222. Defendant failed to provide the legally compliant notice under subdivision (d) of § 1798.82 to Plaintiff and members of the Class Members. On information and belief, to date, associated corporations Account Control Technology Inc. and Account Control Technology Holdings, Inc. have not sent written notice of the data breach to affected individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to Plaintiff and Class Members.

223. On information and belief, many Class Members affected by the breach, have not received any notice at all from Defendant Cerebral in violation of subdivision (d) of § 1798.82.

224. As a result of the violations of § 1798.82, Plaintiff and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

225. As a direct consequence of the actions as identified above, Plaintiff and Class Members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to subdivision (b) of § 1798.84.

Ninth Count

California Unfair Competition Law ("UCL")

Cal. Bus. & Prof. Code § 17200, *et seq*.

(On Behalf of Plaintiff and Class Members)

226. Plaintiff re-alleges and incorporates the allegations of paragraphs 1 through 135, paragraphs 137 through 149, paragraphs 151 through 158, paragraphs 160 through 170, paragraphs 172 through 179, paragraphs 181 through 193, paragraphs 195 through 202, paragraphs 204 through 210, and paragraphs 212 through 225, as if fully set forth.

227. Defendant Cerebral is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

228. Defendant Cerebral violated Cal. Bus. & Prof. Code § 17200 et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

229. Defendant Cerebral's "unfair" acts and practices include:

a. Defendant Cerebral failed to implement and maintain reasonable security measures to protect Plaintiff's and Class Members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of Defendant Cerebral's Data Breach. Defendant Cerebral failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendant Cerebral's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 et seq.), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Defendant Cerebral's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant Cerebral's inadequate security, consumers could not have reasonably avoided the harms that Defendant Cerebral caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

230. Defendant Cerebral has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C.§ 45, and California common law.

231. Defendant Cerebral's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' personal information, which was a direct and proximate cause of the Defendant Cerebral's Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of Defendant Cerebral's Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, which was a direct and proximate cause of Defendant Cerebral's Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' personal information, including by

implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' personal information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150.

232. Defendant Cerebral's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant Cerebral's data security and ability to protect the confidentiality of consumers' personal information.

233. As a direct and proximate result of Defendant Cerebral's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

234. Defendant Cerebral's violations were, and are, willful, deceptive, unfair, and unconscionable.

235. Plaintiff and Class Members have lost money and property as a result of Defendant Cerebral's conduct in violation of the UCL, as stated herein and above.

236. By deceptively storing, collecting, and disclosing their personal information, Defendant Cerebral has taken money or property from Plaintiff and Class Members.

237. Defendant Cerebral acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

238. Plaintiff and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant Cerebral's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

Tenth Count

California Invasion of Privacy

Cal. Const. Art. 1, § 1

(On Behalf of Plaintiff and Class Members)

239. Plaintiff re-alleges and incorporates the allegations of paragraphs 1 through 135, paragraphs 137 through 149, paragraphs 151 through 158, paragraphs 160 through 170, paragraphs 172 through 179, paragraphs 181 through 193, paragraphs 195 through 202, paragraphs 204 through 210, paragraphs 212 through 225, and paragraphs 227 through 238, as if fully set forth.

240. Art. I, § 1 of the California Constitution provides: "All people

are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

241. The right to privacy in California's constitution creates a private right of action against private and government entities.

242. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

243. Defendant Cerebral violated Plaintiff's and Class Members' constitutional right to privacy by collecting, storing, and disclosing their personal information in which they had a legally protected privacy interest, and for which they had a reasonable expectation of privacy, in a manner that was highly offensive to Plaintiff and Class Members, would be highly offensive to a reasonable person, and was an egregious violation of social norms.

244. Defendant Cerebral has intruded upon Plaintiff's and Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential personal information.

245. Defendant Cerebral has intruded upon Plaintiff's and Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential personal information.

246. Plaintiff and Class Members had a reasonable expectation of privacy in that: (i) Defendant's invasion of privacy occurred as a result of Defendant's security practices including the collecting, storage, and unauthorized disclosure of consumers' personal information; (ii) Plaintiff and Class members did not consent or otherwise authorize Defendant Cerebral to disclosure their

personal information; and (iii) Plaintiff and Class Members could not reasonably expect Defendant would commit acts in violation of laws protecting privacy.

247. As a result of Defendant Cerebral's actions, Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant Cerebral's invasion of their privacy and are entitled to just compensation.

248. Plaintiff and Class Members suffered actual and concrete injury as a result of Defendant Cerebral's violations of their privacy interests. Plaintiff and Class Members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant Cerebral's invasions.

249. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as well as disgorgement of profits made by Defendant Cerebral as a result of its intrusions upon Plaintiff's and Class Members' privacy.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class;

b) For equitable relief enjoining Defendant Cerebral from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant Cerebral to utilize appropriate methods and policies with respect to consumer data collection, storage,

and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant Cerebral to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h) For pre- and post-judgment interest on any amounts awarded; and

i) Such other and further relief as this Court may deem just and proper.

Dated: March 17, 2023

Respectfully submitted,

Danielle Perry (SBN 292120)
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
dperry@masonllp.com

/s/ *S. Martin Keleti*
S. Martin Keleti (SBN 144208)
KELETI LAW
9903 Santa Monica Boulevard, Suite 751
Tel: (323) 308-8489
s.martin.keleti@gmail.com
Attorneys for Plaintiff and the Proposed Class

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: March 17, 2023

Respectfully submitted,

Danielle Perry (SBN 292120)
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
dperry@masonllp.com

/s/ *S. Martin Keleti*
S. Martin Keleti (SBN 144208)
KELETI LAW
9903 Santa Monica Boulevard, Suite 751
Tel: (323) 308-8489
s.martin.keleti@gmail.com
Attorneys for Plaintiff and the Proposed Class